(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 11 332 A 1**

(51) Int. Cl.[6]:
G 07 C 9/00
G 06 K 9/62

(21) Aktenzeichen: 198 11 332.3
(22) Anmeldetag: 16. 3. 98
(43) Offenlegungstag: 23. 9. 99

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Meister, Gisela, Dr., 81737 München, DE; Mödl, Albert, Dr., 86368 Gersthofen, DE; Müller, Robert, 83026 Rosenheim, DE; Struif, Bruno, 64287 Darmstadt, DE; Scheuermann, Dirk, 64287 Darmstadt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 196 18 144 C1
WO 97 34 252 A1
DONNERHACKE,Lutz: Fingerabdruck als Eintrittskarte. In: PC Magazin, Jan. 1998, S.260-263;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und Vorrichtung zur Prüfung eines biometrischen Merkmals

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung eines biometrischen Merkmals. Ein Soll-Wert des biometrischen Merkmals wird vorab in Form eines oder mehrerer Datensätze (refdata bzw. refdata 1 und refdata 2) in einem Datenträger (1) gespeichert. Zur Prüfung des biometrischen Merkmals werden zunächst Meßwerte (sens) ermittelt, die einen Ist-Wert des biometrischen Merkmals repräsentieren, und in einem Endgerät (9) bereitgestellt. Der Datenträger (1) übermittelt wenigstens eine Untermenge von ersten Referenzwerten (refdata 1), die von dem Datensatz bzw. den Datensätzen für den Soll-Wert abhängen, an das Endgerät (9). Das Endgerät (9) verknüpft aus den Meßwerten abgeleitete Daten (verdata) mit der Untermenge der ersten Referenzwerte (refdata 1) und übermittelt das Ergebnis der Verknüpfung an den Datenträger (1). Der Datenträger (1) prüft das Ergebnis der Verknüpfung und ermittelt daraus, ob das biometrische Merkmal authentisch ist, d. h. ob der Ist-Wert des biometrischen Merkmals im Rahmen einer zulässigen Toleranzgrenze mit dem Soll-Wert übereinstimmt.

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung eines biometrischen Merkmals.

Biometrische Merkmale werden unter anderem zur Identifizierung bzw. Verifizierung von berechtigten Personen im Zusammenhang mit Zugangs- oder Zugriffskontrollen sowie bei der Durchführung von Finanztransaktionen eingesetzt. So kann mit Hilfe biometrischer Merkmale beispielsweise sichergestellt werden, daß ein Datenträger, wie z. B. eine Chipkarte, die im Rahmen der oben genannten Kontrollen oder Transaktionen zum Einsatz kommt, nur von der dazu berechtigten Person benutzt werden kann, d. h. nur der berechtigten Person wird der Zugang oder Zugriff freigegeben bzw. nur die berechtigte Person kann die Transaktion durchführen. Hierzu wird vor der Freigabe der Benutzung des Datenträgers ein biometrisches Merkmal, wie beispielsweise ein Fingerabdruck, eine Stimmprobe oder die Ausgestaltung des Augenhintergrundes usw. meßtechnisch erfaßt, und nur im Falle eines positiven Vergleichs der Meßwerte mit auf dem Datenträger gespeicherten Referenzwerten wird der Zugang oder Zugriff bzw. die Transaktion des Datenträgers freigegeben. Die Benutzung des Datenträgers findet üblicherweise im Zusammenhang mit einem Endgerät statt, mit dem der Datenträger kommuniziert. Der Vergleich der meßtechnisch erfaßten biometrischen Daten mit gespeicherten Referenzwerten kann prinzipiell sowohl im Datenträger als auch im Endgerät stattfinden. Da die biometrischen Meßdaten häufig sehr umfangreich sind, und auch die Auswertung dieser Daten komplexe Rechenoperationen erfordert, werden hierzu eine hohe Rechenleistung und viel Speicherplatz benötigt. Diese Anforderungen können von heute verfügbaren Datenträgern nicht oder nur bedingt erfüllt werden, so daß die Auswertung der biometrischen Meßdaten in der Regel im Endgerät durchgeführt wird und der Datenträger nur als Speicher für die Referenzwerte dient.

Ein derartiges Endgerät ist aus der DE 44 39 593 C2 bekannt. In diesem Dokument ist eine Vorrichtung zur Zugangs- und Zugriffskontrolle offenbart, die über ein Mikrophon zur Spracherfassung und eine Leseeinrichtung für Chipkarten verfügt. Mit Hilfe des Mikrophons wird eine Sprachprobe aufgenommen und in einer Sprachanalyseeinheit auf sprachtypische Parameter reduziert. Die Sprachparameter werden in einer Auswertungseinheit mit Referenzwerten verglichen, die auf der Chipkarte gespeichert sind und zum Zweck des Vergleichs von der Chipkarte an die Einrichtung zur Zugangskontrolle übertragen werden. Ein Nachteil dieser bekannten Einrichtung besteht darin, daß die auf der Chipkarte gespeicherten Referenzwerte nach außen gegeben werden, und somit die Gefahr bestehen könnte, daß unberechtigte Dritte von diesen Referenzwerten Kenntnis erhalten.

Aus der DE 44 39 593 C2 ist es weiterhin bekannt, daß die Vorrichtung zur Zugangskontrolle, die aus einer Sprachprobe ermittelten Sprachparameter an die Chipkarte weitergibt und die Chipkarte die übermittelten Sprachparameter mit gespeicherten Referenzwerten vergleicht. Diese Vorgehensweise hat zwar den Vorteil, daß die gespeicherten Referenzwerte die Chipkarte nicht verlassen, und somit auch nicht die Gefahr besteht, daß diese von unberechtigten Dritten abgehört werden könnten. Da aber nunmehr an Stelle der Referenzwerte für die Sprachparameter die gemessenen Werte für die Sprachparameter zwischen der Einrichtung und der Chipkarte übertragen werden müssen, besteht die Gefahr, daß statt der Referenzwerte die gemessenen Werte von einem unberechtigten Dritten abgehört werden. Eine Kenntnisnahme der Meßwerte des berechtigten Benutzers durch einen unberechtigten Dritten ist aber von ähnlicher Brisanz wie eine Kenntnisnahme der Referenzwerte.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Prüfung eines biometrischen Merkmals anzugeben, die einen möglichst hohen Sicherheitsstandard bieten und gleichzeitig mit vertretbarem Aufwand zu realisieren sind.

Diese Aufgabe wird durch die Ansprüche 1 und 13 erfüllt.

Um einen möglichst guten Schutz vor dem Mißbrauch, einer mißbräuchlichen Anwendung des Datenträgers zu gewährleisten, ist es erforderlich, daß die Prüfung des biometrischen Merkmals vom Datenträger selbst und nicht etwa von dem Endgerät vorgenommen wird, mit dem der Datenträger im Rahmen seiner bestimmungsgemäßen Anwendung kommuniziert. Ein Problem besteht jedoch insofern, als der Sensor oder die Sensoren zur Erfassung des biometrischen Merkmals in der Regel am Endgerät angebracht ist bzw. angebracht sind, und daher die Meßwerte vom Endgerät zum Datenträger übertragen werden müssen. Ein weiteres Problem besteht darin, daß die Rechen- und Speicherkapazität heute üblicherweise eingesetzter Datenträger, z. B. Chipkarten in der Regel nicht ausreichen, um ausgehend von den Meßwerten des biometrischen Merkmals einen zuverlässigen Vergleich mit Referenzwerten in einer akzeptablen Zeit durchzuführen.

Die Erfindung löst diese Probleme dadurch, daß zum einen sämtliche sicherheitsrelevanten Operationen innerhalb des Datenträgers durchgeführt werden und rechenintensive Operationen ausgelagert werden, soweit die Sicherheit dadurch nicht beeinträchtigt wird, und daß zum anderen im Rahmen dieser Auslagerung vom Datenträger vorgegeben wird, welche Daten in welcher Form vom Endgerät an den Datenträger übermittelt werden. Statt jedes Mal den vollständigen Satz von Meßwerten an den Datenträger zu senden, führt das Endgerät eine Vorauswertung der Meßwerte durch, in deren Rahmen auch eine Verknüpfung von aus den Meßwerten erhaltenen Zwischenergebnissen mit Daten durchgeführt wird, die dem Endgerät von dem Datenträger übermittelt wurden. Nur das Ergebnis dieser Verknüpfung wird dann vom Endgerät an den Datenträger übermittelt, der dann anhand dieser Verknüpfungsergebnisse mit relativ geringem Aufwand feststellen kann, ob das meßtechnisch erfaßte biometrische Merkmal von einem berechtigten Benutzer stammt.

Die Auslagerung von rechenintensiven und nicht sicherheitsrelevanten Operationen vom Datenträger in das Endgerät hat somit den Vorteil, daß der größte Teil des Rechenaufwands im Endgerät anfällt, das dafür entsprechend ausgerüstet werden kann, und nur ein Bruchteil vom Datenträger selbst ausgeführt werden muß, ohne daß es zu einer Verringerung des Sicherheitsstandards kommt. Weiterhin hat die Verknüpfung der Meßwerte mit Daten des Datenträgers vor der Übertragung vom Endgerät zum Datenträger den Vorteil, daß Manipulationsversuche mittels abgehörter Daten wesentlich erschwert werden. So kann der Datenträger beispielsweise seine Vorgaben für die Verknüpfung systematisch oder zufällig variieren und dadurch verhindern, daß eine Manipulation durch Wiedereinspielen der abgehörten Verknüpfungsergebnisse möglich ist. Insbesondere kann durch den Datenträger auch eine jeweils variierende Untermenge der vorausgewerteten Meßwerte ausgewählt werden, so daß ein potentieller Angreifer immer nur Kenntnis von einem Teil der Meßwerte erlangen könnte, und möglicherweise zudem nicht weiß, welcher Teil gerade vom Datenträger ausgewählt wurde.

Zur besseren Veranschaulichung der Erfindung wird diese nachfolgend anhand des biometrischen Merkmals "Fingerabdruck" für ein System, bestehend aus einer Chipkarte und einem Endgerät, erläutert. Das beschriebene Ausführungs-

beispiel stellt dabei nur eine von vielen Realisierungsmöglichkeiten dar. Die Erfindung kann ebenso für beliebige andere biometrische Merkmale, wie beispielsweise Sprache, Augenhintergrund usw. eingesetzt werden. Außerdem können die Details der Realisierung, z. B. welche Charakteristika des biometrischen Merkmals ausgewählt werden und wie diese Charakteristika dargestellt und ausgewertet werden, in weiten Grenzen variieren.

Gemäß dem erfindungsgemäßen Verfahren wird zunächst ein Fingerabdruck meßtechnisch erfaßt, und durch eine geeignete Extraktionsfunktion werden aus den Meßwerten die Charakteristika des Fingerabdrucks ermittelt. Die Charakteristika können beispielsweise in Koordinaten und Art der Minuzien des Fingerabdrucks bestehen. Bei den Minuzien handelt es sich um charakteristische Punkte oder Formen etc. der Fingerabdrucklinien, wie beispielsweise Linienverzweigungen oder Linienendpunkte. Die Chipkarte gibt dem Endgerät z. B. die Koordinaten der aus den Meßwerten ermittelten Minuzien vor, für die die Minuzienarten ausgewertet werden sollen. Das Endgerät verknüpft daraufhin die vorgegebenen Koordinaten mit dem aus den Meßwerten ermittelten Datenmaterial für die Minuzien, ermittelt daraus die Art der an den vorgegebenen Koordinaten ermittelten Minuzien und leitet das Ergebnis an die Chipkarte weiter. Die Chipkarte prüft die übermittelten Minuziendaten und stellt fest, ob das biometrische Merkmal von einem berechtigten Benutzer stammt. Diese Prüfung kann beispielsweise durch Vergleich mit vorab auf der Chipkarte gespeicherten Referenzwerten erfolgen.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindungen werden nachfolgend anhand der in der Zeichnung dargestellten Ausführungsformen beschrieben.

Es zeigen

Fig. 1 eine Chipkarte in Aufsicht,

Fig. 2 ein Blockschaltbild des integrierten Schaltkreises der Chipkarte aus Fig. 1,

Fig. 3 ein Blockschaltbild eines Endgeräts,

Fig. 4 einen stark vergrößerten Ausschnitt aus einem Fingerabdruck,

Fig. 5 einen Datensatz für die Charakteristika eines Fingerabdrucks,

Fig. 6 eine Darstellung des Ablaufs des erfindungsgemäßen Verfahrens,

Fig. 7 eine Darstellung des erfindungsgemäßen Verfahrens unter Zuhilfenahme von Vektoren und Matrizen.

Fig. 1 zeigt eine Chipkarte 1 als ein Beispiel für einen Datenträger in Aufsicht. Die Chipkarte 1 besteht aus einem Kartenkörper 2 und einem Chipmodul 3, das in einer Aussparung des Kartenkörpers 2 angeordnet ist. Das Chipmodul 3 besteht aus einem Kontaktfeld 4 und einem integrierten Schaltkreis 5, der unterhalb des Kontaktfeldes 4 angeordnet ist. Die Abmessungen der Chipkarte 1 sind durch die ISO-Norm 7810 festgelegt und die Funktionsweise des integrierten Schaltkreises 5 ist kompatibel zur ISO-Norm 7816. Die Chipkarte 1 kann beispielsweise als Ausweis für eine Zugangskontrolle zu einem Gebäude vorgesehen sein oder als eine Berechtigungskarte für den Zugang zu einem elektrischen Gerät, beispielsweise einem Computer. Weiterhin kann es sich bei der Chipkarte 1 um eine Bankkarte, eine Kreditkarte, eine Scheckkarte oder ähnliches handeln, mit deren Hilfe Finanztransaktionen durchgeführt werden können.

Neben der in Fig. 1 dargestellten genormten Chipkarte 1 kann die Erfindung auch in Zusammenhang mit anderen Chipkarten oder beliebigen anderen Datenträgern eingesetzt werden, die in der Lage sind, Daten zu speichern.

Die Fig. 2 zeigt ein Blockschaltbild des integrierten Schaltkreises 5 der in Fig. 1 dargestellten Chipkarte 1. Bei dem integrierten Schaltkreis 5 handelt es sich um einen Mikroprozessor, der in der Lage ist, selbständig Berechnungen durchzuführen. Der integrierte Schaltkreis 5 besteht aus einer Zentraleinheit 6, einem Speicher 7 und einer Ein-/Ausgabeeinheit 8. Die Zentraleinheit 6 ist zum Zwecke des Datenaustausches sowohl mit dem Speicher 7 als auch mit der Ein-/Ausgabeeinheit 8 verbunden. Die Zentraleinheit 6 steuert die Funktionsweise des integrierten Schaltkreises 5 und greift dabei in der Regel auf Befehle zurück, die im Speicher 7 abgelegt sind. Der Speicher 7 kann als nichtflüchtiger Speicher, in der Regel ROM oder EEPROM oder als flüchtiger Speicher, RAM ausgeführt sein. In der Regel sind sowohl ein flüchtiger als auch ein nichtflüchtiger Speicher gleichzeitig vorhanden. Die von der Zentraleinheit 6 ausgeführten Befehle sind in der Regel im ROM abgelegt, zum Teil auch im EEPROM. Im EEPROM sind darüber hinaus auch die Referenzwerte für die PIN bzw. für das biometrische Merkmal und weitere für die Anwendung benötigte Daten abgelegt. Der RAM dient als Arbeitsspeicher, in dem gerade benötigte Daten temporär zwischengespeichert werden.

Der Datenaustausch zwischen dem integrierten Schaltkreis 5 und der Außenwelt erfolgt über die Ein-/Ausgabeeinheit 8, die beispielsweise eine serielle Schnittstelle darstellt, und mit dem für die Ein-/Ausgabe von Daten vorgesehenen Kontakt des Kontaktfeldes 4 elektrisch leitend verbunden ist. Für das erfindungsgemäße Verfahren ist es nicht zwingend erforderlich, daß der Datenaustausch zwischen dem integrierten Schaltkreis 5 und der Außenwelt über das Kontaktfeld 4 abgewickelt wird. Statt dessen kann auch eine kontaktlose Chipkarte zum Einsatz kommen, bei der der Datenaustausch nicht über das Kontaktfeld 4 erfolgt, sondern beispielsweise über eine Antennenspule oder über elektrische Koppelflächen.

Obwohl dies in Fig. 1 nicht explizit dargestellt ist, kann die Chipkarte 1 über einen Fingerabdrucksensor zur meßtechnischen Erfassung des Fingerabdrucks verfügen. Dieser Sensor wäre dann an einer geeigneten Stelle des Kartenkörpers 2 angebracht. In der Regel wird der Fingerabdrucksensor jedoch am Endgerät angebracht sein, wie dies in Fig. 3 dargestellt ist, da zur Integration in Chipkarten 1 geeignete Fingerabdrucksensoren derzeit noch nicht oder nur sehr bedingt verfügbar sind.

Fig. 3 zeigt ein Blockschaltbild eines Endgeräts 9, mit dem die Chipkarte 1 in Datenaustausch tritt. Das Endgerät 9 weist einen integrierten Schaltkreis 10 sowie einen Fingerabdrucksensor 11, eine Tastatur 12 und eine Anzeige 13 auf. Der Fingerabdrucksensor 11 kann bei der Variante der Erfindung, bei der die Chipkarte über einen eigenen Fingerabdrucksensor verfügt, entfallen. Der integrierte Schaltkreis 10 des Endgeräts 9 weist in Analogie zum integrierten Schaltkreis 5 der Chipkarte 1 eine Zentraleinheit 14 auf, die mit einem Speicher 15 und einer Ein-/Ausgabeeinheit 16 verbunden ist. Weiterhin ist die Zentraleinheit 14 auch mit dem Fingerabdrucksensor 11, mit der Tastatur 12 und der Anzeige 13 verbunden.

Mit Hilfe des Fingerabdrucksensors 11 kann ein Fingerabdruck des Benutzers meßtechnisch erfaßt werden. Die so ermittelten Daten können dann in der Zentraleinheit 14 weiterverarbeitet werden und das Ergebnis dieser Verarbeitung kann über die Ein-/Ausgabeeinheit 16 an die entsprechende Ein-/Ausgabeeinheit 8 des integrierten Schaltkreises 5 der Chipkarte 1 übermittelt werden. Ebenso kann die Zentraleinheit 14 über die beiden Ein-/Ausgabeeinheiten 8 und 16 Daten vom integrierten Schaltkreis 5 der Chipkarte 1 empfangen. Über die Tastatur 12 kann der Benutzer für die jeweilige Anwendung benötigte Daten manuell eingeben. Welche Dateneingabe jeweils erforderlich ist, kann dabei

auf der Anzeige 13 angezeigt werden.

Um eine mißbräuchliche Verwendung der Chipkarte 1 durch einen unberechtigten Dritten zu verhindern, beispielsweise bei Verlust- oder Diebstahl der Chipkarte 1 ist die Benutzung der Chipkarte 1 nur nach einer zuvor erfolgten positiven Identifizierung bzw. Verifizierung eines biometrischen Merkmals des Benutzers, im folgenden Beispiel des Fingerabdrucks, möglich. Die Identifizierung über ein biometrisches Merkmal ersetzt oder ergänzt die bei Chipkarten 1 übliche Authentifizierung des Benutzers durch Eingabe einer geheimen persönlichen Identifikationsnummer (PIN). Ein Referenzwert für diese Identifikationsnummer ist im Speicher 7 des integrierten Schaltkreises 5 von außen unzugänglich gespeichert und wird mit der eingegebenen Identifikationsnummer verglichen. Analog hierzu sind bei der Erfindung im Speicher 7 des integrierten Schaltkreises 5 Referenzwerte für das biometrische Merkmal gespeichert, auf die bei einer Prüfung der Meßwerte zurückgegriffen wird. Fällt der PIN-Vergleich bzw. die Prüfung des biometrischen Merkmals positiv aus, so wird die Chipkarte 1 für die Benutzung freigegeben. Andernfalls werden in der Regel noch eine bestimmte Anzahl von weiteren Versuchen zugelassen und falls auch diese Versuche nicht positiv verlaufen, wird die Chipkarte gesperrt.

Fig. 4 zeigt einen stark vergrößerten Ausschnitt aus einem Fingerabdruck. Der Fingerabdruck setzt sich aus einer Reihe von mehr oder weniger stark geschwungenen Linien zusammen, die innerhalb des gezeigten Ausschnitts als durchgehende Linie verlaufen, sich verzweigen oder einen Endpunkt aufweisen. Für die Fingerabdruckprüfung können beispielsweise die Koordinaten der Verzweigungen und der Endpunkte als zu prüfende Charakteristika herangezogen werden, da ein derartiger Datensatz ein individuelles Merkmal der Person darstellt, von der der Fingerabdruck stammt. Um die Koordinaten der Charakteristika des Fingerabdrucks zu ermitteln, wurde der in Fig. 4 dargestellte Ausschnitt des Fingerabdrucks mit einem Koordinatensystem versehen, und es wurden beispielhaft die Koordinaten x1 und y1 einer Linienverzweigung 17 sowie die Koordinaten x2 und y2 eines Linienendpunktes 18 eingezeichnet. Ein kompletter Datensatz für einen Fingerabdruck besteht aus einer ganzen Reihe solcher Koordinatenpaare, für die zudem jeweils die Art des Charakteristikums (Verzweigung, Endpunkt, gegebenenfalls weitere) angegeben ist. Die Struktur eines derartigen Datensatzes ist in Fig. 5 dargestellt.

Fig. 5 zeigt eine mögliche Struktur eines Datensatzes refdata, der die Charakteristika eines Fingerabdrucks repräsentiert. Die erste Zeile der in Fig. 5 dargestellten Zahlenmatrix gibt die laufende Nummer der einzelnen Koordinatenpaare an. In der zweiten und der dritten Zeile werden die x- und y-Koordinate zur Festlegung der Positionen der Charakteristika des Fingerabdrucks aufgeführt. In der vierten Zeile wird jeweils durch einen Wert z für die einzelnen Koordinatenpaare angegeben, von welcher Art die Charakteristika des Fingerabdrucks sind, d. h. ob es sich jeweils um eine Verzweigung oder um einen Endpunkt usw. handelt. Der Datensatz besteht aus insgesamt n Einträgen, wobei jeder Eintrag vier Werte (laufende Nummer, x-Koordinate, y-Koordinate, Art des Charakteristikums) umfaßt.

In Fig. 6 ist das erfindungsgemäße Verfahren zur Prüfung eines Fingerabdrucks dargestellt. Auf der linken Seite der Fig. 6 sind die Verfahrensschritte dargestellt, die im Endgerät 9 durchgeführt werden und auf der rechten Seite die Verfahrensschritte, die im Datenträger und damit im vorliegenden Beispiel in der Chipkarte 1 durchgeführt werden. Die Pfeile zwischen der linken und rechten Seite der Fig. 6 deuten einen Datentransport zwischen Endgerät 9 und Chipkarte 1 an.

Im Vorfeld des erfindungsgemäßen Prüfverfahrens, beispielsweise bei der Personalisierung der Chipkarte 1 durch den Kartenherausgeber, werden in der Chipkarte 1 eine Reihe von Daten und mathematischen Funktionen gespeichert, die für die Durchführung des Verfahrens benötigt werden. Wie weiter unten noch im Einzelnen beschrieben, hängt es von der Ausführungsform der Erfindung ab, um welche Daten es sich dabei im Einzelnen handelt. Verfahrensschritte, die für eine Ausführungsform spezifisch sind, sind in Fig. 6 durch den Buchstaben A für eine erste Ausführungsform und durch den Buchstaben B für eine zweite Ausführungsform gekennzeichnet.

Das eigentliche Prüfverfahren beginnt mit der Erfassung des Fingerabdrucks des Karteninhabers durch das Endgerät 9. Hierzu ist es erforderlich, daß der Karteninhaber einen Finger, beispielsweise den Zeigefinger auf den Fingerabdrucksensor 11 des Endgeräts 9 auflegt. Die Trennung zwischen der Initialisierung und der Prüfung im engeren Sinn wird in Fig. 6 durch eine waagrechte Linie verdeutlicht. Die im Rahmen der Fingerabdruckerfassung ermittelten Meßwerte des Fingerabdrucks werden durch den Datensatz sens repräsentiert. Das Format und genaue Aussehen dieses Datensatzes sens spielt für die weitere Betrachtung keine Rolle. Wichtig ist lediglich, daß das Endgerät 9 über ein Funktion calc verfügt, mit der aus dem Meßdatensatz sens ein Datensatz verdata ermittelt werden kann, der in seiner Struktur dem Datensatz refdata entspricht, d. h. im Datensatz verdata sind für den aktuell gemessenen Fingerabdruck die Koordinaten und die Art der Charakteristika des Fingerabdrucks vermerkt.

In einem nächsten Schritt übermittelt die Chipkarte 1 einen Datensatz refdata1 an das Endgerät. Der Datensatz refdata1 wurde zuvor, ebenso wie ein Datensatz refdata2 aus dem Datensatz refdata ermittelt, indem auf den Datensatz refdata eine Extraktionsfunktion extr1 bzw. extr2 angewendet wird. Die Speicherung von refdata 1 und refdata2, insbesondere aber refdata wird üblicherweise in verschlüsselter Form erfolgen. Bezüglich der Einzelheiten zur Ermittlung der Datensätze refdata1 und refdata2 ist zwischen zwei Ausführungsformen der Erfindung zu unterscheiden.

Gemäß einer ersten Ausführungsform (Buchstabe A) ist der Datensatz refdata, dessen Format in Fig. 5 abgebildet ist, komplett in der Chipkarte 1 gespeichert. Dieser Datensatz wurde beispielsweise vorab von der kartenherausgebenden Stelle aus Meßdaten des Fingerabdrucks des zukünftigen Karteninhabers erzeugt und im Speicher 7 der Chipkarte 1 abgelegt. Die Extraktionsfunktionen extr1 und extr2 werden immer dann auf den Datensatz refdata angewendet, wenn der Datensatz refdata1 bzw. refdata2 benötigt wird und nicht bereits verfügbar ist. Im Falle des hier beschriebenen Beispiels einer Fingerabdruckprüfung anhand von Charakteristika des Fingerabdrucks beschreibt der Datensatz refdata1 die Koordinaten x und y der Charakteristika des Fingerabdrucks, die geprüft werden sollen. Der Datensatz refdata2 beschreibt jeweils die Art der Charakteristika für die einzelnen Koordinaten. Mit anderen Worten, der Datensatz refdata1 weist die Zeilen 1 bis 3 des in Fig. 5 dargestellten Datensatzes refdata auf und der Datensatz refdata2 die Zeilen 1 und 4. Dabei ist insbesondere noch darauf hinzuweisen, daß der Datensatz refdata1 und als Folge davon auch der Datensatz refdata2 in der Regel nicht alle laufenden Nummern des Datensatzes refdata umfassen, d. h. die Datensätze refdata1 und refdata2 repräsentieren jeweils nur eine Untermenge der im Datensatz refdata jeweils mit einer laufenden Nummer versehenen einzelnen Charakteristika des Fingerabdrucks. Dies ist für das im Folgenden beschriebene erfindungsgemäße Verfahren von großer Bedeutung, da mit Hilfe des Datensatzes refdata1 ausgewählt werden kann, welche Charak-

teristika des Fingerabdrucks geprüft werden sollen.

Bei einer zweiten Ausführungsform (Buchstabe B) der Erfindung ist der Datensatz refdata nicht in der Chipkarte 1 gespeichert. Statt dessen sind lediglich die aus ihm abgeleiteten Datensätze refdata1 und refdata2 im Speicher 7 der Chipkarte 1 gespeichert. Die gespeicherten Datensätze refdata1 und refdata2 werden in diesem Fall in der Regel jedoch sämtliche laufende Nummern des Datensatzes refdata umfassen, und es wird dann jeweils erst bei der Fingerabdruckprüfung aus diesen vollständigen Datensätzen refdata1 und refdata2 jeweils eine Untermenge für die Prüfung ausgewählt.

Das Bereitstellen der Datensätze refdata1 und refdata2 kann somit sowohl gemäß der ersten Ausführungsform durch Extrahieren und Bilden von Untermengen aus dem gespeicherten Datensatz refdata als auch gemäß der zweiten Ausführungsform durch Bilden von Untermengen aus den gespeicherten Datensätzen refdata1 und refdata2 erfolgen. In jedem Fall handelt es sich bei den für das weitere Verfahren verwendeten Datensätzen refdata1 und refdata2 um die Untermengen, die durch Auswählen bestimmter laufender Nummern hervorgegangen sind und in der Regel somit nicht mehr um Datensätze, die alle laufenden Nummern aufweisen.

Für das vorliegende Beispiel bedeutet die Übermittlung des Datensatzes refdata1 von der Chipkarte 1 an das Endgerät 9, daß die Chipkarte 1 dem Endgerät 9 mitteilt, für welche Koordinaten der gemessene Fingerabdruck auf seine Charakteristika hin geprüft werden soll.

Die Auswahl der zu prüfenden Charakteristika, die von der Chipkarte 1 getroffen wird, kann nach unterschiedlichen Kriterien vorgenommen werden. So kann im Sinne einer möglichst effizienten und zuverlässigen Prüfung versucht werden, besonders signifikante bzw. deutlich erkennbare Charakteristika auszuwählen. Weiterhin kann die Auswahl zufallsbedingt oder nach einer geheimen Systematik variiert werden, um einen Mißbrauch durch Abhören der übertragenen Daten durch unberechtigte Dritte zu verhindern oder zumindest zu erschweren. Weiterhin kann die Auswahl auch von der aktuellen Anwendung abhängen, so daß beispielsweise bei einer Anwendung, in deren Rahmen nur geringe Geldbeträge transferiert werden und somit im Betrugsfall nur ein geringer Schaden angerichtet werden kann, eine geringere Anzahl von Charakteristika ausgewählt wird, als in einem Fall, bei dem höhere Beträge transferiert werden. Auf diese Art und Weise kann der getriebene Aufwand jeweils sehr gut an den erforderlichen Sicherheitsstandard angepaßt werden. Um einen Angriff generell zu erschweren, ist es in allen Fällen natürlich auch möglich, daß der Datensatz refdata1 und auch weitere zwischen der Chipkarte 1 und dem Endgerät 9 übermittelte Daten in verschlüsselter Form übertragen werden.

Im Endgerät 9 wird der übertragene Datensatz refdata1 mit Hilfe einer Funktion f mit dem Datensatz verdata verknüpft und auf diese Art und Weise ein Datensatz verdata2 erzeugt. Anschaulich gesprochen, wird für jedes der mit dem Datensatz refdata1 übertragenen Koordinatenpaare die Art des Charakteristikums des Fingerabdrucks ermittelt. Der so ermittelte Datensatz verdata2 gibt somit jeweils für die vorgegebenen Koordinaten die Art des gefundenen Charakteristikums an bzw. eine bestimmte Art der Codierung, die besagt, daß für spezielle vorgegebene Koordinaten kein Charakteristikum ermittelt werden konnten, und weist somit die Zeilen 1 und 4 der Matrix aus Fig. 5 auf. Die Berechnung der Funktion f wäre in einer Chipkarte 1 aufgrund von Speicher- und/oder Zeitkomplexität nicht oder nur mit erheblichem Mehraufwand möglich, da die Funktion f auch ein Ähnlichkeitsverfahren beinhaltet.

Anschließend wird der Datensatz verdata2 vom Endgerät 9 an die Chipkarte 1 übertragen. Die Chipkarte 1 prüft den Datensatz verdata2 und abhängig vom Ergebnis dieser Prüfung wird der Fingerabdruck als authentisches biometrisches Merkmal akzeptiert oder auch nicht. Bei der Prüfung kann es sich beispielsweise um einen Vergleich des aus der Messung ermittelten Datensatzes verdata2 mit dem Referenzdatensatz refdata2 handeln. Dieser Vergleich kann so durchgeführt werden, daß für jede laufende Nummer des Referenzdatensatzes refdata2 die Art des Charakteristikums des Fingerabdrucks mit dem entsprechenden Wert eines aus den Meßwerten ermittelten Datensatzes verdata2 verglichen wird. Der gemessene Fingerabdruck kann dann als authentisch akzeptiert werden, wenn zum einen die Anzahl der gefundenen Charakteristika im Datensatz verdata2 entweder absolut oder prozentual einen vorgebbaren Schwellwert überschreitet und zum anderen die Übereinstimmung zwischen den Datensätzen verdata2 und refdata2 einen weiteren vorgebbaren Schwellwert überschreitet. Die dazu erforderlichen Vergleichsoperationen lassen sich mit relativ geringem Rechen- und Speicheraufwand durchführen und sind dadurch von der Chipkarte 1 problemlos abwickelbar. Daneben können auch eine Vielzahl anderer Auswerteverfahren eingesetzt werden. So kann beispielsweise die Auswertung der Anzahl der gefundenen Charakteristika völlig unterbleiben und es kann lediglich die Übereinstimmung zwischen den Datensätzen verdata2 und refdata2 geprüft werden, wobei in diese Prüfung in der Regel die Anzahl der gefundenen Charakteristika insofern eingeht, als für jedes nicht gefundene Charakteristikum eine Nichtübereinstimmung festgestellt wird.

Neben der geschilderten Einsatzmöglichkeit im Zusammenhang mit einer Fingerabdruckprüfung läßt sich das erfindungsgemäße Verfahren auch bei anderen biometrischen Merkmalen einsetzen, beispielsweise zum Prüfen von Sprachproben oder von Messungen des Augenhintergrunds usw.

Das dem erfindungsgemäßen Verfahren zugrundeliegende Prinzip läßt sich in allgemeinerer Form unter Zuhilfenahme von mathematischen Symbolen beschreiben. Bei dieser Beschreibung wird davon ausgegangen, daß die biometrischen Daten, und zwar sowohl Meßwerte als auch Referenzwerte, nach einer gewissen Vorverarbeitung in Form von Vektoren vorliegen. Diese Vektoren werden als x (Meßwerte) und y (Referenzwerte) bezeichnet. Im Rahmen des erfindungsgemäßen Verfahrens wird auf der Basis eines Vergleichs der beiden Vektoren x und y ermittelt, ob das gemessene biometrische Merkmal mit großer Wahrscheinlichkeit authentisch ist. Eine relativ einfache Möglichkeit des Vergleichs besteht in der Berechnung des Euklidischen Abstandes. Alternativ zu diesem Vergleichsverfahren kann auch die Norm über positiv definite Matrizen gebildet werden, und auf diese Art und Weise der Vektor x der Meßwerte mit den Vektor y der Referenzwerte verglichen werden. Hierzu wird zunächst der Differenzvektor z aus den Vektoren x und y gebildet und dann die Norm des Vektor z gemäß der Formel

$$\|z\|^2 = z^T A z$$

gebildet. Die Matrix A dient dazu, die einzelnen Komponenten des Differenzvektors z unterschiedlich stark zu gewichten.

Damit gemäß dem erfindungsgemäßen Verfahren eine Arbeitsteilung zwischen dem Endgerät und dem Datenträger vorgenommen werden kann, wird die Matrix A in eine orthogonale Matrix T und eine Diagonalmatrix D aufgespalten, so daß gilt:

$A = T^T D T$.

Somit ergibt sich das Quadrat der Norm zu:

$$\|z\|^2 = z^T T^T D T z$$
$$= (Tz)^T D (Tz)$$
$$= (Tx - Ty)^T D(Tx - Ty)$$
$$= (Tx - Ty)^T D(Tx - Ty)$$
$$= \sum_{i=1}^{n} d_{ii} (Tx - Ty)_i^2,$$

wobei d_{ii} die Diagonalelemente der Matrix D darstellen.

Unter Berücksichtigung dieser Aufspaltung wird das erfindungsgemäße Verfahren durchgeführt, indem die Matrix A für die Gewichtung und der Vektor y für die Referenzwerte vorgegeben werden. Daraus werden durch geeignete Funktionen die orthogonale Matrix T, das Produkt aus der orthogonalen Matrix T und dem Referenzvektor y und die Diagonalmatrix D ermittelt und im Datenträger 1 gespeichert.

Die Vorgehensweise bei einer Prüfung des biometrischen Merkmals ist in **Fig. 7** dargestellt. Entsprechend **Fig. 6** sind auch bei **Fig. 7** die im Endgerät **9** durchgeführten Schritte auf der linken Bildseite dargestellt und die im Datenträger durchgeführten Schritte auf der rechten Bildseite. Voraussetzung für das erfindungsgemäße Verfahren ist, daß die Matrizen T und D sowie das Produkt aus der Matrix T und dem Referenzvektor y vorab im Datenträger **1** gespeichert wurden. Das eigentliche Prüfverfahren beginnt damit, daß das biometrische Merkmal vom Endgerät **9** erfaßt wird. Das Ergebnis dieser Datenerfassung ist der Datensatz sens. Aus dem Datensatz sens wird unter Zuhilfenahme einer geeigneten Funktion calc der Vektor x der Meßwerte ermittelt. Anschließend übermittelt der Datenträger **1** die orthogonale Matrix T an das Endgerät **9**. Im Endgerät **9** wird das Produkt aus der Matrix T und dem Vektor x gebildet und an den Datenträger **1** übermittelt. Zur Berechnung der Norm des Differenzvektors z sind im Datenträger **1** lediglich noch Multiplikationen mit einer Diagonalmatrix erforderlich, so daß der Datenträger **1** zur Berechnung der Norm des Vektors z bei einer quadratischen Matrix der Dimension n letztendlich nur n Multiplikationen bzw. Quadrierungen durchführen muß. Würde man die Norm des Vektors z direkt und ohne Übertragung der orthogonalen Matrix T an das Datenendgerät **9** berechnen, wären im Datenträger n^2 Multiplikationen erforderlich, d. h. durch das erfindungsgemäße Verfahren kann der Rechenaufwand im Datenträger **1** erheblich reduziert werden. Auch bei dieser allgemeinen Vorgehensweise werden sämtliche sicherheitsrelevanten Operationen im Datenträger **1** durchgeführt. Die an das Datenendgerät **9** übertragene orthogonale Matrix T hängt zwar vom Vektor y der Referenzdaten ab, reicht aber nicht zur Rekonstruktion des Vektors y aus. Die bezüglich der Sicherheit kritische Diagonalmatrix D verbleibt im Datenträger **1**.

Patentansprüche

1. Verfahren zur Prüfung eines biometrischen Merkmals mit den Schritten
   - Ermitteln von Meßwerten (sens), die einen Ist-Wert des biometrischen Merkmals repräsentieren und Bereitstellen dieser Meßwerte in einem Endgerät **9**,
   - Übermitteln wenigstens einer Untermenge von ersten Referenzwerten (refdata1), die von einem vorab festgelegten Soll-Wert des biometrischen Merkmals abhängen, von einem Datenträger an das Endgerät,
   - Verknüpfen von aus den Meßwerten (sens) abgeleiteten Daten (verdata) mit der Untermenge der ersten Referenzwerte (refdata1) im Endgerät (9),
   - Übermitteln des Ergebnisses der Verknüpfung (verdata2) vom Endgerät (9) an den Datenträger (1) und
   - Prüfen des Ergebnisses der Verknüpfung im Datenträger (1).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Meßwerte (sens) mit Sensormitteln des Endgeräts (9) ermittelt werden.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Meßwerte (sens) mit Sensormitteln des Datenträgers (1) ermittelt werden.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die ersten Referenzwerte (refdata1) und zweite Referenzwerte (refdata2) im Datenträger (1) aus einem gespeicherten Referenzdatensatz (refdata), der den Soll-Wert des biometrischen Merkmals repräsentiert, ermittelt werden.
5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die ersten Referenzwerte (refdata1) und zweite Referenzwerte (refdata2) vorab aus einem Referenzdatensatz (refdata), der den Soll-Wert des biometrischen Merkmals repräsentiert, ermittelt werden und im Datenträger (1) gespeichert werden.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Ermittlung der ersten Referenzwerte (refdata1) aus dem Referenzdatensatz (refdata) derart durchgeführt wird, daß eine Rückrechnung von den ersten Referenzwerten (refdata1) auf den Referenzdatensatz (refadata) nicht möglich ist.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Untermenge der ersten Referenzwerte (refdata1) unter Zuhilfenahme einer Zufallsgröße variiert wird.
8. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Untermenge der ersten Referenzwerte (refdata1) nach einem geheimen Verfahren systematisch variiert wird.
9. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Untermenge der ersten Referenzwerte (refdata1) bei Einsatz des Datenträgers für finanzielle Transaktionen vom Transaktionsbetrag abhängt.
10. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Untermenge der ersten Referenzwerte (refdata1) von dem vorab festgelegten Soll-Wert des biometrischen Merkmals abhängt.
11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die aus den Meßwerten (sens) abgeleiteten Daten (verdata) Charakteristika des biometrischen Merkmals darstellen.
12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Ergebnis (verdata2) der Verknüpfung der aus den Meßwerten (sens) abgeleiteten Daten (verdata) mit der Untermenge der ersten Referenzwerte (refdata1) unter Zuhilfenahme von im Datenträger (1) gespeicherten zweiten Referenzwerten (refdata2) geprüft wird.
13. System zur Prüfung eines biometrischen Merk-

mals, bestehend aus einem Datenträger (1) und einen Endgerät (9), dadurch gekennzeichnet, daß

- das Endgerät (9) Meßwerte (sens), die einen Ist-Wert des biometrischen Merkmals repräsentieren, bereitstellt,
- daß der Datenträger (1) wenigstens eine Untermenge von ersten Referenzwerten (refdata1), die von einem vorab festgelegten Soll-Wert des biometrischen Merkmals abhängen, an das Endgerät (9) übermittelt,
- das Endgerät (9) von aus den Meßwerten (sens) abgeleitete Daten (verdata) mit der Untermenge der ersten Referenzwerte (refdata1) verknüpft,
- daß das Endgerät (9) das Ergebnis der Verknüpfung an den Datenträger (1) übermittelt und
- daß der Datenträger (1) das Ergebnis der Verknüpfung prüft.

14. System nach Anspruch 13, dadurch gekennzeichnet, daß der Datenträger (1) eine Chipkarte ist.

Hierzu 5 Seite(n) Zeichnungen

Nummer: DE 198 11 332 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 23. September 1999

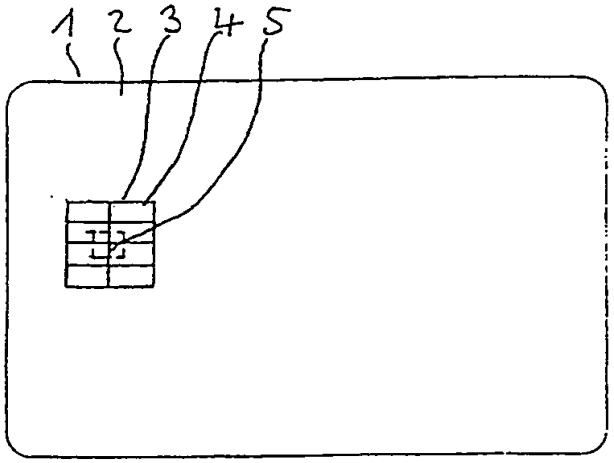

Fig. 1

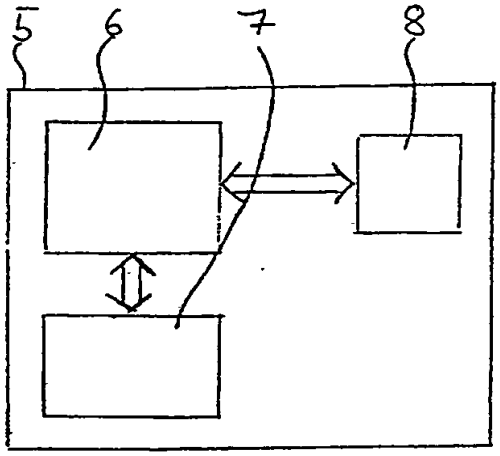

Fig. 2

Nummer: DE 198 11 332 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 23. September 1999

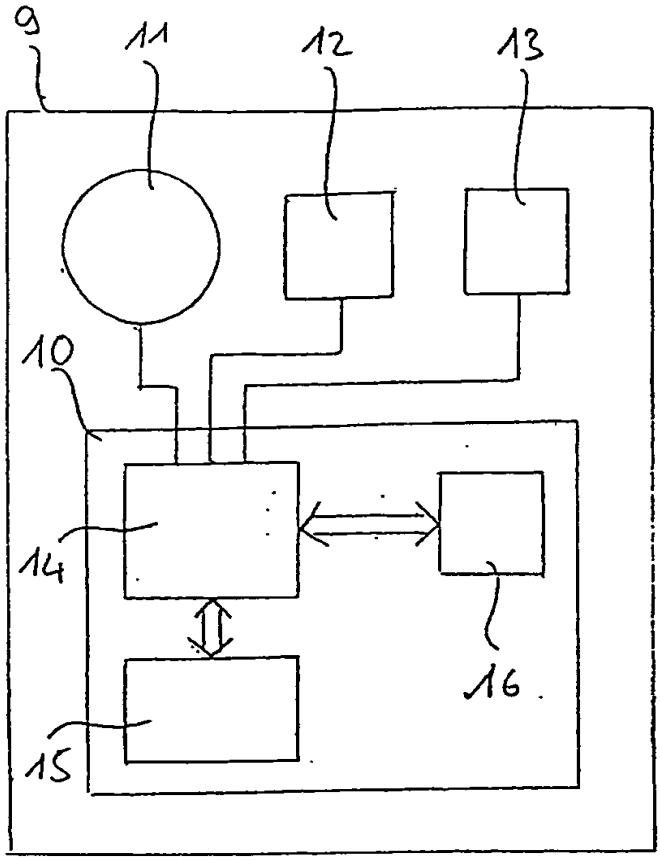

Fig. 3

Nummer: DE 198 11 332 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 23. September 1999

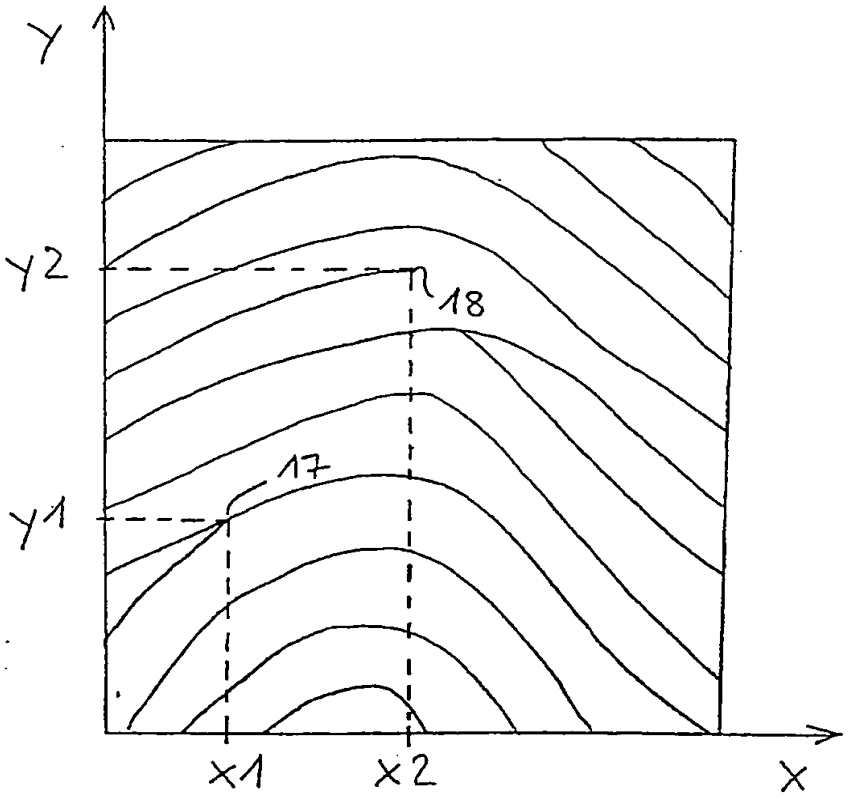

Fig. 4

1	2	3	••••	n
x1	x2	x3	••••	xn
y1	y2	y3	••••	yn
z1	z1	z3	••••	zn

Fig. 5

Nummer: DE 198 11 332 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 23. September 1999

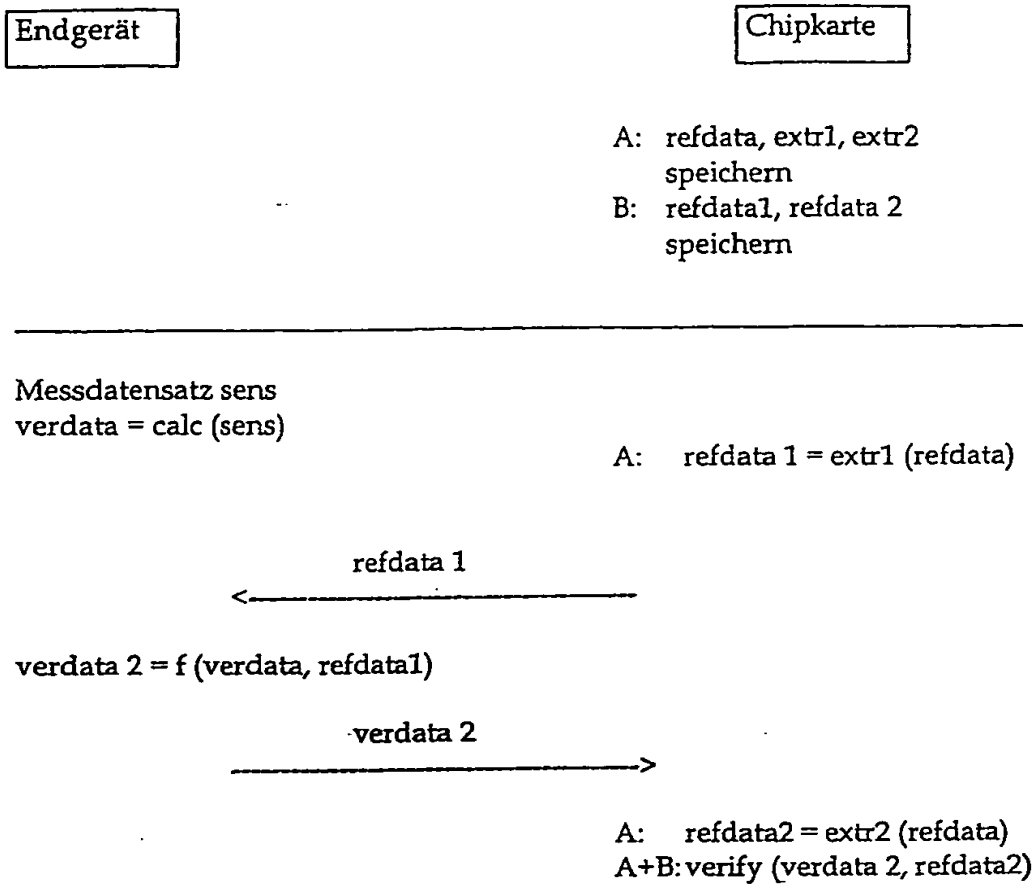

Fig. 6

Nummer: DE 198 11 332 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 23. September 1999

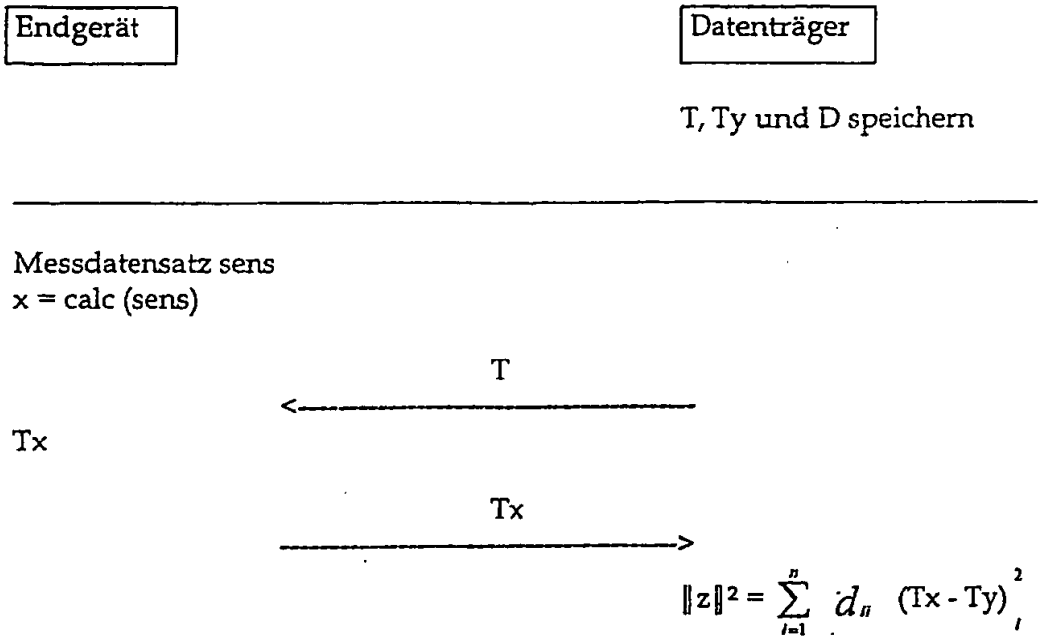

Fig. 7

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.